Translation of Citation 2

----Omitted----

One-Way Hash Function:

One-way hash function satisfies the following essential conditions:

- It is impossible to inversely convert an output value to an input value.
- A slight difference between inputs arises a large difference between outputs.
- A size of an output is constant regardless a size of input.
- When inputs are different to each other, their outputs are seldom the same.

In Fig. 2, a message "M" means a password in a password system. Although the length of the password is not naturally limited, it is limited by actualizing a system.

What are realized using the one-way hash function? It is important that when a password is treated or processed with the one-way hash function, the password cannot be obtained from inverse treatment of the treated value. That is, if the value obtained by treating the password with the one-way hash function (the value is referred to "an encrypted password) is published, the original password is not obtained therefrom. Therefore, information is kept secret.

How is it demonstrated or evaluated whether a character sequence inputted from a user is the password? In order to demonstrate it, the character sequence inputted is treated with the one-way hash function, and then the treated value is compared with the encrypted password. When they are the same, the input character sequence is the password. Accordingly, only when the input sequence and the password are the same, the input sequence is validated.

MD5

Linux incorporates a command "md5sum" by default. The command uses "MD5" as an algorism of the one-way hash function. Using MD5, a content of a standard input or file is processed to provide its hash

value. The size of the hash value of MD5 is 128 bits. Using the nature of the one-way hash function, it is possible to check whether or not the content of the file is corrupted.